REMARKS

Claims 1, 2, and 4-23 are pending in this application.

Applicants have amended claims 1, 2, 4, 8, 11, 13, and 15-19, and have added new claims 20-23. In addition, Applicants have canceled claim 3.

The changes to the claims made herein do not introduce any new matter. In particular, the element that the identification information is non-confidential finds support at least in Paragraph [0033] of the published specification (see US 2007/0185811 A1). The element that the user identification corresponds to, or has been derived from, the identification information finds support at least in Paragraph [0037]. The element that the secret data pertains to a secret that is known to the user finds support at least in Paragraph [0014]. The element that the presentation of the secret to the user signals to the user that the terminal can be trusted finds support at least in Paragraphs [0015] and [0046]. The elements of new claims 20-23 find support at least in Paragraph [0020].

Rejection Under 35 U.S.C. § 101

Claims 18 and 19 have been rejected under 35 U.S.C. § 101 as being directed toward non-statutory subject-matter. In support of the rejection, the Examiner states in Paragraph 7 of the Office Action that the non-physical medium mentioned in Paragraph [0025] of the published specification (see US 2007/0185811 A1) could be interpreted as a transitory, propagating signal.

Without any admission as to the propriety of the rejection, and solely to expedite allowance of the subject application, Applicants have amended claims 18 and 19 to specify that the computer program product comprises a physical medium. Paragraph [0025] of the published specification states that such a physical medium may be, as a non-limiting example, a semiconductor memory or a diskette or a CD-ROM. Applicants submit that a computer program product that comprises a physical medium, as presently claimed, clearly constitutes statutory subject matter. Accordingly, Applicants request that the rejection of claims 18 and 19 under 35 U.S.C. § 101 be withdrawn.

Rejection under 35 U.S.C. § 112

Applicants respectfully request reconsideration of the rejection of claims 1-19 under 35 U.S.C. § 112, second paragraph, as being indefinite (as noted above, claim 3 has been canceled).

Without any admission as to the propriety of the rejection, and solely to expedite allowance of the subject application, Applicants have amended claims 1, 2, 4, 8, 11, 13, and 15-19.

Referring to Paragraph 10 of the Office Action, the identification information has been linked to the user identification data that is contained in the terminal data by the recitation that "the user identification data corresponds to, or has been derived from, the identification information determined by the terminal."

Referring to Paragraphs 11 and 12 of the Office Action, the Examiner's suggestions regarding the terms "terminal data" and "feature data" have been adopted. Furthermore, the term "transmission data" has been used in claims 8, 13, 16, 17, and 19.

Referring to Paragraphs 13 and 14 of the Office Action, the claims have been amended to recite that the secret is presented to the user.

Referring to Paragraphs 15 and 16 of the Office Action, the allegedly unclear wording has been clarified.

Referring to Paragraph 17 of the Office Action, the structure of the background system with various modules has been clarified in claim 16. Claim 15 has been amended in a similar manner.

Referring to Paragraph 18 of the Office Action, the structure of the background system and the terminal(s) with various modules has been clarified in claim 17.

Referring to Paragraph 19 of the Office Action, the wording related to the performing of the transaction has been adapted to the wording of present claim 1. The component that is adapted for the recited operation, namely a sixth module that is a module of the terminal, has been recited in claim 17.

Referring to Paragraph 20 of the Office Action, the allegedly unclear wording has been removed from claim 17.

Accordingly, Applicants request that the rejection of claims 1, 2, and 4-19 under 35 U.S.C. § 112, second paragraph, be withdrawn.

<u>Rejection Under 35 U.S.C. § 103</u>

Claims 1-19 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over *Lai On* (US 2002/0059531 A1) in view of *Schneier* (Handbook of Applied Cryptography) (as noted above, claim 3 has been canceled).

Applicants respectfully request reconsideration of the obviousness rejection. As will be explained in more detail below, the combination of the *Lai On* and *Schneier* references would not have rendered the subject matter defined in claims 1, 2, and 4-23, as presented herein, obvious to a person having ordinary skill in the art.

<u>Independent Claims</u>

In the field of electronic transactions, a user typically authorizes a transaction by entering a personal feature at a terminal. The personal feature may be, for example, a PIN or a fingerprint. However, a possible attacker might set up a counterfeit terminal that looks confusingly like a genuine terminal, but records and misappropriates the user's personal feature data. For example, incidents have been reported in which counterfeit ATM machines were set up so that they fraudulently collected account information from the inserted cards and recorded the associated PINs that were entered by unsuspecting users.

The present invention therefore addresses the problem of allowing a user to reliably convince himself/herself of the integrity of a terminal before the user needs to present any personal feature to the terminal.

To solve the above problem, the terminal of the present invention initially only determines non-confidential identification information. The terminal then sends this non-confidential information, in the form of terminal data, to the background system. The terminal data serves to authenticate the terminal at the background system. If the authentication of the terminal at the background system has been successful, then the terminal receives secret data from the background system, wherein the secret data pertains to a secret that is known to the user. This secret serves to signal to the user that the terminal can be trusted.

Lai On neither teaches nor suggests at least the claimed elements that are underlined in the above paragraph. First, *Lai On* does not teach that its identification information is non-confidential, as claimed. To the contrary, Paragraph [0020] of *Lai On* discloses that the identification information can include (1) a user ID and a user password, or (2) a user biometric. In both cases, the identification information includes confidential elements, namely the password or the user biometric. Paragraph [0021] of *Lai On* further makes it clear that "the authentication site verifies the identification information and generates a user session key and a second site key." This means that *Lai On* requires the user to submit his or her full – and confidential – credentials to the first vendor site as the very first step of *Lai On*'s process. However, the first vendor site is not necessarily trustworthy and may in fact just be trying to steal the user's confidential password or user biometric. The user has no way of verifying whether or not the first vendor site can be trusted before entering confidential information. Thus, the system of *Lai On* has exactly those problems that are addressed by the present invention.

The claimed non-confidential identification information can also not be linked to *Lai On*'s user session key for at least the reason that *Lai On*'s user session key is clearly confidential. Knowledge of this user session key permits access to any one of the second vendor sites, and therefore the user session key must be treated confidentially exactly in the same way as a password or a fingerprint. However, Paragraph [0022] of *Lai On* discloses that the user is required to log into the second vendor site by transmitting the user session key to this second vendor site as the very first step of the user's interaction with the second vendor site, i.e., before the integrity of the second vendor site has been proved.

Second, *Lai On* does not teach any authentication of the terminal at the background system. In this respect, the Office Action cited in section 24, item (c) the words "*Verifies the Identification Information*" from Figure 3, box 303 of *Lai On*. However, the identification information of *Lai On* is information that comes from the user and that is merely forwarded by first vendor site to the authentication site. The step of verifying the identification information therefore at most represents an authentication of the user at the authentication site, and not an authentication of the terminal, as claimed.

Third, *Lai On* does not teach any secret data that pertains to a secret that is known to the user, wherein the secret serves to signal to the user that the terminal can be trusted. Neither the user session key nor the second site key of *Lai On* are secret data. This has been acknowledged by the Examiner in Paragraph 25 of the Office Action. Perhaps more importantly, neither the user session key nor the second site key serves to signal to the user that any one of the first and second vendor sites can be trusted. As indicated in Paragraph [0021] of *Lai On*, the background system generates the user session key and the second site key in response to the verification of the user-supplied identification information. This does not imply any checking of the integrity of the first vendor site. With respect to the second vendor site, Paragraph [0022] of *Lai On* discloses that the second vendor site receives the user session key from the user and forwards it to the authentication site. The authentication site then verifies the received user session key by comparing it to a stored user session key. In case of a successful verification, the authentication site transmits the second site key to the verified user through the second site. Thus the transmission of the second site key just indicates that the verification of the session key at the authentication site was successful. It does not imply any verification of the second vendor site, and it does not indicate anything about the trustworthiness of the second vendor site. A counterfeit second vendor site could easily obtain the user session key from the user, forward the user session key to the verification site, receive the second site key from the verification site, and forward the second site key to the user. Consequently, *Lai On* does not disclose any secret that signals to the user that a certain terminal can be trusted.

Applicants further note that the Examiner's line of argumentation in Paragraph 24 of the Office Action is not fully consistent with the use of the word "terminal" in the independent claims. In all independent claims, the word "terminal" is introduced by the indefinite article "a," and is then always referred to using the definite article "the." This makes it clear that all elements of the independent claims that refer to the terminal actually refer to one and the same terminal. However, in Paragraph 24, item (a) of the Office Action, the Examiner identifies the terminal with *Lai On*'s first vendor site, but in Paragraph 24, item (e) of the Office Action, the Examiner refers to step 305 of Figure 3 of *Lai On*, which is apparently a step performed by *Lai On*'s second vendor site. Consider, for example, claim 1, in which all steps are recited as "steps performed by the terminal." To show that these steps are known from *Lai On*, the Examiner would have needed to show that one of *Lai On*'s two vendor sites (i.e., either the first vendor site or the second vendor site) performs all these steps. However, in Paragraph 24 of the present Office Action, the Examiner refers to a mixture of some steps performed by the first vendor site and other steps performed by the second vendor site. This is clearly not sufficient. Corresponding observations apply with respect to the other independent claims.

Summing up, the present invention strives to protect the user's confidential personal feature date (such as a PIN or a fingerprint) from being spied out by a fraudulent terminal. In complete contrast, *Lai On* discloses a process in which the very first step requires the user to log into the non-verified first vendor site by entering confidential information (such as a user password or a user biometric) at the first vendor site. Similarly, when the user wishes to access the second vendor site, he or she is required give the confidential user session key to the non-verified second vendor site. The present invention can certainly not be regarded as obvious from the system of *Lai On* that is in no way concerned about the invention's object of protecting the user's confidential information from being spied out by possibly fraudulent sites.

The *Schneier* reference does not cure any of the above-discussed deficiencies of the *Lai On* reference relative to the claimed subject matter.

Accordingly, independent claims 1, 8, 13, and 15-19, as presented herein, are patentable under 35 U.S.C. § 103(a) over the combination of *Lai On* in view of *Schneier*.

Dependent Claims

Each of dependent claims 2, 4-7, 20, and 21 depends from independent claim 1. Each of dependent claims 9-12, 22, and 23 ultimately depends from independent claim 8. Dependent claim 14 depends from independent claim 13. All of the present dependent claims are therefore patentable under 35 U.S.C. § 103(a) over the combination of *Lai On* in view of *Schneier* for at least the reason that each of these claims ultimately depends from one of the present independent claims.

Further, present claim 2 recites that "the terminal data is secured with at least one of a MAC and a cryptographic signature for authentication at the background system." In Paragraph 27 of the Office Action, the Examiner rejected the former version of claim 2, referring to the words "*User Session Key*" that are shown in Figure 3, box 305 of *Lai On*. However, there is no disclosure in *Lai On* that the user session key (which is likely just a character sequence) is secured with at least one of a MAC and a cryptographic signature, as claimed.

Still further, new claims 20-23 recite that the secret (1) is easily identified by the user, or (2) is at least one of a displayed image, an acoustic output, and tactile information. Both *Lai On*'s user session key and *Lai On*'s second site key can be assumed to be string of characters, as acknowledged by the Examiner in Paragraph 29 of the Office Action. Furthermore, such keys are typically long and random-looking character strings. Such keys are neither easily identified by the user, nor are they at least one of a displayed image, an acoustic output, and tactile information, as claimed.

Conclusion

In view of the foregoing, Applicants respectfully request reconsideration and reexamination of claims 1, 2, and 4-19, as amended herein, and examination of claims 20-23, and submit that these claims are in condition for allowance. Accordingly, a notice of allowance is respectfully requested. In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at **(408) 749-6902**. If any additional fees are due in connection with the filing of this paper, then the

Commissioner is authorized to charge such fees to Deposit Account No. 50-0805 (Order No. WACHP011).

Respectfully submitted,
MARTINE PENILLA & GENCARELLA, L.L.P.

/Peter B. Martine/

Peter B. Martine
Reg. No. 32,043

710 Lakeway Drive, Suite 200
Sunnyvale, California 94085
Customer Number 25920